

ABSTRACT

5 A method for restoring a computer system modified by malicious code. The method scans the computer system for the malicious code, identifies the malicious code and retrieves from a data file, information relating to the malicious code including at least one command used for restoring the computer system to a state that existed prior to modification by the malicious code. The at least one command is executed to restore the computer system to substantially the state as it existed prior to modification by the malicious code.